Efficient algorithms for Riemann–Roch spaces

GRÉGOIRE LECERF

CNRS & École polytechnique, France

Joint work with SIMON ABELARD (Thales SIX GTS, France)
ELENA BERARDINI (CNRS, France)
ALAIN COUVREUR (Inria, France)

Partly funded by the French “Agence de l'innovation de défense”

Recent Trends in Computer Algebra 2023, IHP Paris

September 26, 2023

Motivation

At present time…

- Riemann–Roch spaces are difficult to compute in general.
- Practical applications are restricted to a few families of curves with explicit Riemann–Roch spaces.
- Riemann–Roch spaces are involved in more and more applications in computer science.

Goals

- Have an asymptotically reasonably fast algorithm.
- Have software implementations able to handle curves of degree a few thousands over finite fields.
- Speed-up the algorithms for $\mathbb{F}_2$ and some usual families of curves.

Applications

Error correcting codes

GOPPA (1977) for ordinary curves

TSFASMAN, VLĂDUŢ, and ZINK (1982), explicit constructions that beat random codes

Secret sharing

CHEN and CRAMER (2006)

Resilience in distributed storage systems

BARG, TAMO, and VLĂDUŢ (2017)

Secure multi-party computations and zero-knowledge proofs

BORDAGE, LHOTEL, NARDI, and RANDRIAM (2022)

...

Algebraic curves

- $\mathbb{K}$ is a field.
- $F \in \mathbb{K}[x, y, z]$ is an absolutely irreducible homogeneous polynomial.
- $\mathbb{P}^2$ is the projective plane over $\bar{\mathbb{K}}$.
- The set of zeros of F in $\mathbb{P}^2$ is written $\mathcal{C}$.
- The set of rational functions defined on $\mathcal{C}$ over $\mathbb{K}$ is written $\mathbb{K}(\mathcal{C})$, that is

$$\mathbb{K}(\mathcal{C}) := \left\{ \frac{A}{B} : A \text{ and } B \text{ are homogenous, } B \text{ is prime to } F, \deg A = \deg B \right\} / \sim$$

where $A/B \sim A'/B' \iff AB' - A'B \in (F)$.

Valuation at a regular point

- $\zeta = (\zeta_x : \zeta_y : \zeta_z)$ is a regular point on $\mathcal{C}$.
- Up to a linear change of variables, we assume that $\zeta_z = 1$ and $\frac{\partial F}{\partial y}(\zeta) \neq 0$.
- By the implicit function theorem, $\mathcal{C}$ is locally defined by a power series

$$\varphi(x) := \zeta_y + c_1(x - \zeta_x) + c_2(x - \zeta_x)^2 + \cdots \in \bar{\mathbb{K}}[[x - \zeta_x]]$$

that satisfies $F(x, \varphi(x), 1) = 0$.

If $G/H \in \mathbb{K}(\mathcal{C})$, then its valuation at ζ is defined by

$$\mathrm{val}_\zeta(G/H) := \mathrm{val}_{x-\zeta_x}(G(x, \varphi(x), 1) / H(x, \varphi(x), 1))$$

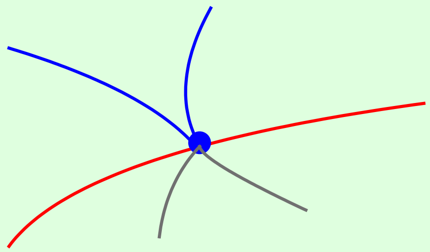
This is independent of the coordinates.

Valuations at a singular point

Up to a (random) change of coordinates: $\zeta = (0:0:1)$ and $F(x,y,1)$ is monic in y.

$F(x,y,1)$ locally factorizes into

$$F(x,y,1) = u(x,y)\, f_1(x,y)\, f_2(x,y) \cdots f_n(x,y),$$



where u is a unit in $\mathbb{K}[[x,y]]$ and $f_i \in \mathbb{K}[[x]][y]$ is monic and irreducible, for $i = 1, \ldots, n$.

The valuation val_x of $\mathbb{K}((x))$ extends uniquely to a valuation v_i of $\mathbb{K}((x))[y]/(f_i)$, of valuation group $r_i^{-1}\mathbb{Z}$.

Let $A \in \mathbb{K}[x,y,z]$ be homogeneous and prime to F.

$$\mathrm{Div}_\zeta A := r_1 v_1(A)\, \mathfrak{P}_1 + \cdots + r_n v_n(A)\, \mathfrak{P}_n$$

$\mathfrak{P}_i$ is a symbol, called a place $\equiv f_i(x,y)$ independently of the coordinates.

Computational problem: obtain $f_1, \ldots, f_n$ and $v_1, \ldots, v_n$ efficiently.

Divisors

$A, B \in \mathbb{K}[x,y,z]$ are prime to F.

$$\mathrm{Div}(A) := \sum_{F(\zeta)=A(\zeta)=0} \mathrm{Div}_\zeta(A) \qquad \mathrm{Div}(A/B) := \mathrm{Div}(A) - \mathrm{Div}(B)$$

Generally a divisor $D = \sum_{\mathfrak{P}} c_{\mathfrak{P}} \mathfrak{P}$ is a finite $\mathbb{Z}$-combination of places of $\mathcal{C}$.

$$\sum_{\mathfrak{P}} c_{\mathfrak{P}} \mathfrak{P} \leqslant \sum_{\mathfrak{P}} c'_{\mathfrak{P}} \mathfrak{P} \quad \Longleftrightarrow \quad \forall \mathfrak{P}, c_{\mathfrak{P}} \leqslant c'_{\mathfrak{P}}$$

D is said to be positive (also called effective) whenever $D \geqslant 0$.

The degree of a divisor is defined by:

$$\deg\left(\sum_{\mathfrak{P}} c_{\mathfrak{P}} \mathfrak{P}\right) := \sum_{\mathfrak{P}} c_{\mathfrak{P}}$$

Riemann–Roch spaces

Given a divisor D of $\mathcal{C}$, we want to compute a $\mathbb{K}$-basis of the Riemann–Roch space

$$\mathcal{L}(D) := \left\{ \frac{A}{B} \in \mathbb{K}(\mathcal{C}) \setminus \{0\} : \mathrm{Div}(A/B) \geqslant -D \right\} \cup \{0\}.$$

Example 1. $\deg D < 0 \Longrightarrow \mathcal{L}(D) = \{0\}$

Notation: $D = D_+ - D_-$, where D_+ and D_- are *positive* with disjoint supports.

Dense input size $\approx (\deg F)^2 + \deg D_+$

Example 2. $\mathbb{K} := \mathbb{F}_2$, $F(x,y,z) := y^3 + x^3 + y^2 z$, $D = \mathfrak{P}$, where $\mathfrak{P}$ is the place of $\mathcal{C}$ at the regular point $\zeta := (0:1:1)$.

$$\mathcal{L}(D) = \left\langle 1, \frac{y}{x} \right\rangle \text{ has dimension 2.}$$

Around ζ and for $z = 1$: $y = 1 + x^3 + O(x^4)$, $v_\zeta(1) = 0$ and $v_\zeta\left(\frac{y}{x}\right) = -1$.

Known algorithms

Arithmetic algorithms. Derived from the work of HENSEL and LANDBERG (1902)

COATES (1970), DAVENPORT (1981)

HESS (2002): deterministic, polynomial time, state-of-the-art algorithm.

Implemented in the MAGMA and SINGULAR computer algebra system.

Integral closures are the first bottleneck: sharp bounds given by ABELARD (2020).

Geometric algorithms. Derived from the work of BRILL and NOETHER (1874, for ordinary curves only)

LE BRIGAND and RISLER (1988) for general curves.

HACHÉ (1996, PhD) for an implementation in Axiom.

HUANG and IERARDI (1994): $O((\deg F)^{6\omega} \deg D_+)$ for ordinary curves, $O((\deg F \deg D_+)^{2\omega})$ for smooth curves and rational support for D.

($\omega \equiv$ feasible complexity exponent for matrix multiplication)

Known algorithms — continued

VOLCHECK (1994): use of Puiseux series for char. 0

CAMPILLO and FARRÁN (2002): Hamburger–Noether expansions for char. >0

KHURI-MAKDISI (2007): additions in the Jacobian of general genus-g curves in time $\tilde{O}(g^{\omega})$

LE GLUHER and SPAENLEHAUER (2020): modern computer algebra techniques, fast C++ implementation for nodal curves, heuristic $\tilde{O}(((\deg F)^2 + \deg D_+)^{\omega})$

ABELARD, COUVREUR, and LECERF (2022): for ordinary curves

$$\tilde{O}\left(((\deg F)^2 + \deg D_+)^{\frac{\omega+1}{2}}\right) \text{ “operations”}$$

ABELARD, BERARDINI, COUVREUR, and LECERF (2022): today's talk

$$\tilde{O}(((\deg F)^2 + \deg D_+)^{\omega})$$

for general curves in char. zero or $>\deg F$.

The Brill–Noether algorithm for a line

Problem. $F(x,y,z)=y$, $\alpha_1,\dots,\alpha_n$ are distinct values in $\mathbb{K}$, $m_1,\dots,m_n$ are in $\mathbb{Z}$

$$D := m_1\,(\alpha_1:0:1) + \cdots + m_n\,(\alpha_n:0:1)$$

Solution. Easy in this case!

1. $H(x,y,z) := \prod_{i=1,m_i>0}^{n} (x-\alpha_i z)^{m_i}$ is a common denominator for $\mathcal{L}(D)$.
2. $G(x,y,z) := \prod_{i=1,m_i<0}^{n} (x-\alpha_i z)^{-m_i}$ and $G_i(x,y,z) := z^{l-i} x^i G$ for $i=0,\dots,l$, where

$$l := \deg H - \deg G = \deg D.$$

Finally, $G_0/H,\dots,G_l/H$ is a basis of $\mathcal{L}(D)$.

The Brill–Noether method

Algorithm

Input. An absolutely irreducible plane projective curve $\mathcal{C}$ defined over $\mathbb{K}$ by the equation $F=0$, and a $\mathbb{K}$-rational divisor D of $\mathcal{C}$.

Output. A $\mathbb{K}$-basis of $\mathcal{L}(D)$.

1. Compute the adjoint divisor $\mathcal{A} := \mathrm{Div}(\mathrm{d}x) - \mathrm{Div}\left(\frac{\partial F}{\partial y}\right)$ of $\mathcal{C}$.
2. Find a homogeneous polynomial $H \in \mathbb{K}[x,y,z]$ prime to F such that
$$\mathrm{Div}(H) \geqslant D + \mathcal{A}.$$
3. Compute $\mathrm{Div}(H) - D$.
4. Compute a $\mathbb{K}$-basis $G_1, \dots, G_l$ of the space of all homogeneous polynomials $G \in \mathbb{K}[x,y,z]$ of degree $\deg H$ such that $\mathrm{Div}(G) \geqslant \mathrm{Div}(H) - D$.
5. Return $G_1/H, \dots, G_l/H$.

Overview of the complexity analysis

Task	Complexity
1. Adjoint divisor $\mathcal{A}$	$\tilde{O}((\deg F)^3)$
2. Denominator H of $\mathcal{L}(D)$	$\tilde{O}(((\deg F)^2 + \deg D_+)^\omega)$
3. $\mathrm{Div}(H) - D$	$\tilde{O}(((\deg F)^2 + \deg D_+)^2)$
4. Numerator basis $G_1, \ldots, G_l$	$\tilde{O}(((\deg F)^2 + \deg D_+)^\omega)$

Theorem. [ABELARD, BERARDINI, COUVREUR, LECERF]

- $\mathcal{L}(D)$ *can be computed by a probabilistic algorithm of Las Vegas type with an expected number of* $\tilde{O}(((\deg F)^2 + \deg D_+)^\omega)$ *operations in* $\mathbb{K}$*, whenever* $\mathrm{char}\, \mathbb{K} = 0$ *or* $> \deg F$*.*

  $\mathbb{K}$ *is algebraically closed of characteristic zero and roots of univariate polynomials are "for free", then the cost drops to* $\tilde{O}\left(((\deg F)^2 + \deg D_+)^{\frac{\omega+1}{2}}\right)$*.*

- *If the curve has only ordinary singularities then the cost drops to* $\tilde{O}\left(((\deg F)^2 + \deg D_+)^{\frac{\omega+1}{2}}\right)$ *for any characteristic.*

Task 1. Adjoint divisor

1. Apply a random linear change of coordinates.
2. Solve $F(x,y,1) = \frac{\partial F}{\partial y}(x,y,1) = 0$.

   $\mathbb{K} = \mathbb{F}_q$. Use VILLARD's bivariate system solver (2023) with quasi-linear time.

   Otherwise. Use classical resultant and gcd, with directed evaluation (VAN DER HOEVEN, LECERF, 2020), in time $\tilde{O}((\deg F)^3)$.

3. Compute the rational Puiseux expansions at each solution.
   For all Puiseux expansion $X(t), Y(t)$, of ramification index r, compute

$$\mathrm{val}_t\left(\frac{r\,t^{r-1}}{\frac{\partial F}{\partial y}(X(t), Y(t), 1)}\right)$$

   char 0 or $>\deg F$. Use the algorithm by POTEAUX and WEIMANN (2021), in time $\tilde{O}((\deg F)^3)$.

   Ordinary curves. Ad hoc method in time $\tilde{O}((\deg F)^3)$.

Task 3. $\mathrm{Div}(H)$

By construction

- H is a common denominator of $\mathcal{L}(D)$, $\deg_y H < \deg F$;
- $\mathrm{Div}(H) \geqslant \mathcal{A} + D$;
- There exists a smooth divisor R such that $\mathrm{Div}(H) = \mathcal{A} + R$;
- $d := \deg H$ satisfies $d \deg F = O((\deg F)^2 + \deg D_+)$.

This is made possible thanks to the Riemann–Roch theorem.

Algorithm

1. Solve $H(x,y,1) = F(x,y,1) = 0$ outside the singular locus of $\mathcal{C}$.

   As before, in time $\tilde{O}(((\deg F)^2 + \deg D_+)^{1.5})$, and faster over finite fields.

2. For all solutions ζ compute $\mathrm{val}_\zeta H$.

Tasks 2 and 4. Vanishing conditions

General problem: compute bases of bivariate polynomials satisfying certain degree bounds and vanishing conditions.

Vanishing condition: $(\Delta(b), \mu(a), X(t), Y(t), m)$

1. A truncation order $m \in \mathbb{N}_{>0}$.

2. A rational Puiseux expansion

$$\mathbb{K} \underset{\text{separable}}{\subseteq} \mathbb{K}[\beta] := \mathbb{K}[b]/(\Delta(b)) \underset{\text{separable}}{\subseteq} \mathbb{K}[\alpha,\beta] := (\mathbb{K}[\beta])[a]/(\mu(a))$$

   $(X(t), Y(t)) \in (\mathbb{K}[\alpha,\beta][[t]]/(t^m))^2$, with $X(t) = \beta + \gamma t^r$, γ invertible in $\mathbb{K}[\alpha,\beta]$, and r is the ramification index.

We say that a polynomial $g \in \mathbb{K}[x,y]$ satisfies this vanishing condition when

$$\mathrm{val}_t(g(X(t), Y(t))) \geqslant m.$$

Tasks 2 and 4. Vanishing polynomials

Unknowns: polynomials $g \in \mathbb{K}[x,y]$ such that

$$\deg_y g < \deg F \text{ and } \deg g \leqslant d := \deg H.$$

The number of unknowns is $\simeq d \deg F = O((\deg F)^2 + \deg D_+)$

Linear equations: $g \in \mathbb{K}[x,y]$ satisfies several vanishing conditions

$$((\Delta_i(b), \mu_i(a), X_i(t), Y_i(t), m_i))_{i=1,\ldots,e}$$

The number of linear equations is

$$\sigma := \sum_{i=1}^{e} m_i \deg \Delta_i \deg \mu_i = O((\deg F)^2 + \deg D_+)$$

Problem: Find a $\mathbb{K}$-basis of the solutions g.

First method: direct linear system solving

$$\tilde{O}((d\deg F + \sigma)^{\omega}) = \tilde{O}(((\deg F)^2 + \deg D_+)^{\omega})$$

Second method: structured polynomial matrices

Compute a $\mathbb{K}[x]$-basis of the polynomials $g \in \mathbb{K}[x][y]$ such that $\deg_y g < \deg F$ that satisfy the vanishing conditions.

JEANNEROD, NEIGER, SCHOST, VILLARD. Computing minimal interpolation bases. *J. Symbolic Comput.*, 83:272–314, 2017.

Simplified from Theorem 1.4. Let $s := (\deg F - 1, \deg F - 2, \ldots, 1, 0)$. A basis in s-Popov form can be computed in time

$$\tilde{O}(\sigma^{\omega}\lceil \deg F / \sigma \rceil) = \tilde{O}(((\deg F)^2 + \deg D_+)^{\omega})$$

$\mathbb{K}[x]$-bases are smaller.

Split case. $\mathbb{K}$ is algebraically closed of characteristic zero and is endowed with a routine that computes the roots of any polynomial $\theta \in \mathbb{K}[x]$ in softly linear time.

Theorem 1.5 of "Computing minimal interpolation bases", by JEANNEROD, NEIGER, SCHOST, VILLARD, *J. Symbolic Comput.*, 83:272–314, 2017.

Let $s := (\deg F - 1, \deg F - 2, \ldots, 1, 0)$. A basis in s-Popov form can be computed in time

$$\tilde{O}((\deg F)^{\omega-1}(\sigma + (\deg F)^2)) = \tilde{O}\left(((\deg F)^2 + \deg D_+)^{\frac{\omega+1}{2}}\right)$$

$\mathcal{C}$ only admits ordinary singularities.

Theorem 1.4 of "Fast computation of shifted Popov forms of polynomial matrices via systems of modular polynomial equations" by NEIGER, *ISSAC'16*.

A basis in s-Popov form can be computed in time

$$\tilde{O}((\deg F)^{\omega-1}((\deg F)^2 + \deg D_+)) = \tilde{O}\left(((\deg F)^2 + \deg D_+)^{\frac{\omega+1}{2}}\right)$$

Future work

hardness ↓

- Extend the complexity exponent ω for any positive characteristic and any curve.
- Avoid generic linear change of coordinates, at least in practice.
- Achieve a software implementation that can handle curves of degree a few thousands over finite fields.
- Speed up the algorithms for special families of curves.
- Extend the complexity exponent $(\omega+1)/2$ to more curves: the bottle-neck mostly lies in structured linear algebra.

References

- ABELARD, COUVREUR, and LECERF. Efficient computation of Riemann–Roch spaces for plane curves with ordinary singularities. *Applicable Algebra in Engineering, Communication and Computing*, 2022.
- ABELARD, BERARDINI, COUVREUR, and LECERF. Computing Riemann–Roch spaces via Puiseux expansions. *Journal of Complexity*, 73:101666, 2022.
- BERARDINI, COUVREUR, and LECERF. A proof of the Brill–Noether method from scratch. Technical Report, HAL, 2022.

Thank you for your attention!